UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,819	10/31/2001	Richard Paul Tarquini	10017333-1	4711

7590   08/26/2005

HEW LETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO   80527-2400

EXAMINER
ALOMARI, FIRAS B

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 June 2005*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All   b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
   application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1.   Applicant's arguments, see Amendment, filed 06/13/2005, with respect to the rejection(s)of claim(s) 12 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made.

2.   The objection to the specifications is withdrawn as the application contained blanks with reference to related applications, but is remedied by filling them in.

3.   The applicant's arguments regarding claim 1 is not persuasive. As Vaidya discloses monitoring all seven layers of the OSI model see Col 4 Lines 28-33. And further it is commonly known in the art that the OSI model includes seven layers (physical, Data Link, Network, Transport, Session, Presentation, Application) which includes the present invention's network stack.

4.   The applicant's argument regarding claims 6 & 13 are not persuasive. As Vaidya discloses comparing the packet with a plurality of machine-readable network-exploit signatures to see if the packet matches any of the known signatures Col 6, Line 57 through Col 7, Line 10. Claims 1 & 6 are more specific as they disclose "in response to detecting said data addressed to said network object, **accessing a subset of attack signature profiles** corresponding to said network object **based on said correspondence data**; and

executing at least one attack signature profile included in **said subset corresponding to said**

network object to determine if said data addressed to said network object is associated with

a network intrusion attempt" the attack profile in Vaidya's invention includes the

machine-readable network-exploit signatures of the present invention.

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2.   Claims 1-5 & 13-15 are rejected under 35 U.S.C. 102(e) as being anticipated by

Vaidya US (6,279,113).

As per claim 1: Vaidya discloses a node of a network maintaining an instance of an

intrusion prevention system, the node comprising:

A memory module for storing data in machine-readable format for retrieval and

execution by a central processing unit; (Item 39 of FIG. 2 and Col 6, Lines 53-56) and

An operating system comprising a network stack comprising a protocol driver, (Items

30,34 and 36 of FIG2. and Col 6, Lines 11-18)

A media access control driver and an instance of the intrusion prevention system implemented as an intermediate driver and bound to the protocol driver and the media access control driver, (Col 7, Lines 12-24)

the intrusion prevention system comprising an associative process engine and an input/output control layer, the input/output control layer operable to receive at least one of a plurality of machine-readable network-exploit signatures from a database and provide the at least one machine-readable network-exploit signatures to the associative process engine,(Col 7, lines 24-36, and Col 6, lines 7-11)

the associative process engine operable to compare a packet with the at least   one machine-readable network-exploit signature and determine a correspondence between the packet and the at least one machine-readable network-exploit signature. (Col 6, Lines 18-21 and Col 7, Lines 32-36)

As per claim 2: Vaidya discloses the method of claim 1, wherein the database is maintained in storage device of the node. (Col 6, lines 3-7)

As per claim 3: Vaidya discloses the node according to claim 1, wherein each of the plurality of machine-readable network-exploit signatures comprise a respective directive that defines instructions to be executed upon determination of a correspondence between the packet and the respective exploit signature.(Col 6, Lines 18-26)

As per claim 4: Vaidya discloses the node according to claim 1, wherein, upon

determination of a correspondence between the packet and two or more of the plurality

of machine-readable network-exploit signatures, each of the directives of the two or

more machine-readable network-exploit signatures are executed by the intrusion

prevention system. (Col 7, Line 47 through Col 8 line 15)

As per claim 5: Vaidya discloses the node according to claim 1, wherein, upon

determination of a correspondence between the packet and two or more of the plurality

of machine-readable network-exploit signatures, an alternative directive is executed, the

alterative directive dependent upon the combination of the two or more network-exploits

signatures having a correspondence with the packet.(Col 9, Line 62 through Col 10

Line 16 and Col 11 lines 5-14)

As per claim 13: Vaidya discloses a computer-readable medium having stored thereon

set of instructions to be executed, the set of instructions, when executed by a

processor, cause the processor to perform a computer method of:

comparing a packet with a plurality of machine-readable network-exploit signatures;(

Col 6, Line 57 through Col 7 Line 6)

determining a correspondence between the packet and at least a subset of the plurality

of machine-readable network-exploit signatures; and (Col 6, Lines 57-63)

generating a record of the subset with which the correspondence is made.(Col 7, Lines

8-11 / the reaction module takes steps to trace the session associated with the

packet.......)

As per claim 14: Vaidya discloses the computer readable medium according to claim

13, further comprising a set of instructions that cause, when executed by the processor,

the processor to perform a computer method of:

determining a correspondence between the packet and a subset of the plurality

of machine-readable network-exploit signatures (*Col 6, Line 57 through Col 7 Line 6*),

each machine-readable network-exploit signature comprising a directive; and executing,

by the processor, each directive of the record of machine-readable signatures. *(Col 7,*

Lines 24-45)

As per claim 15 Vaidya discloses the computer readable medium according to claim 13,

further comprising a set of instructions that cause, when executed by the processor, the

processor to perform a computer method of executing a directive dependent on the

machine-readable network-exploit signatures within the subset. (*Col 6, Lines 18-26)*

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.   Claims 6-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Vaidya US (6,279,113) in view of Shanklin et al. US (6,578,147).

As per claim 6: Vaidya discloses a method of analyzing a packet at a node of a network

by an intrusion prevention system executed by the node, comprising:

reading the packet by the intrusion prevention system; (Col 6, lines 57-59 and item 58 of

FIG. 3)

comparing the packet with a plurality of machine-readable network-exploit

signatures; and (Col 6, Line 57 through Col 7 Line 6)

but Vaidya doesn't explicitly show determining a correspondence between the packet

and at least two of the network-exploit signatures. However Shanklin disclose an

intrusion detection system comprising intrusion detection sensors that forward packets

from different sessions to a network analyzer to be used in detecting certain types of

composite signatures (Col 5, Lines 29-39). Therefore it would be obvious to one with

ordinary skill in the art the time the invention was made to modify Vaidya system with

the teaching Shanklin to include a step for determining the correspondence between

packet and at least two signatures. One would be motivated to do so in order to enable the system to detect correlations among signatures in different sessions(Col 6, Lines 4-8).

As per claim 7: Vaidya discloses the method according to claim 6, further comprising generating a record of the at least two of the plurality of machine-readable network-exploit signatures with which a correspondence with the packet is made. (Col 8, Lines 44-53)

As per claim 8: Vaidya discloses the method according to claim 7, further comprising transmitting the record to a management node connected to the network. (Col 5, Lines 47-51)

As per claim 9: Vaidya discloses the method according to claim 7, further comprising logging the record in a database. (Col 9, Lines 21-26)

AS per claim 10: Vaidya discloses the method according to claim 6, further comprising executing, by the intrusion protection system, a respective directive of each of the at least two machine-readable signatures determined to correspond with the packet. (Col 7, Line 47 through Col 8 line 15)

AS per claim 11: Vaidya discloses the method according to claim 6, further comprising

executing, by the intrusion protection system, at least one directive of the machine-

readable network exploit signatures of the record determined to have a correspondence

with the packet. (Col 9, Line 62 through Col 10 Line 16 and Col 11 lines 5-14).

As per claim 12: Vaidya discloses the method according to claim 6, further comprising

executing, by the intrusion protection system *(Col 7, Lines 24-45)*, an alternative

directive dependent on the record of machine-readable signatures determined to have a

correspondence with the packet *(Col 6, Lines 18-26 & Col 6, Line 57 through Col 7 Line

6)*.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Firas Alomari whose telephone number is (571) 272-

7963. The examiner can normally be reached on M-F from 8:30 am - 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, AYAZ SHEIKH can be reached on (571) 272-3795. The fax phone number

for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Firas Alomari
Examiner
Art Unit 2136

FA

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100